POL-20090701A

STATEWIDE INFORMATION SECURITY POLICY

Information Security Programs

Approved

Office of the Chief Information Officer

Department of Administration
Information Technology Services Division
PO Box 200113
Helena, MT 59620-0113
Tel: (406) 444-2700
FAX: (406) 444-2701

March 5, 2010

Brian Schweitzer
Governor

State of Montana

DEPARTMENT OF ADMINISTRATION
Janet R. Kelly, Director

CHIEF INFORMATION OFFICER
Richard B. Clark

APPROVED STATEWIDE POLICY: INFORMATION SECURITY PROGRAMS

EFFECTIVE DATE: JULY 1, 2012
APPROVED: MARCH 5, 2010

I. Purpose

This **Information Security Programs Policy** (Policy) establishes the requirement to implement Information Security Programs processes and actions within agencies.

II. Authority

The Montana Information Technology Act requires that information technology be appropriately secured. See §2-17-534, MCA. The Chief Information Officer is responsible for statewide policies for security of information technology.

This Policy may conflict with other instruments currently in effect. Where conflicts exist, the more restrictive instrument governs. The development of future policies or standards will explicitly identify and retire any superseded portions of current policies or standards.

III. Policy Statement

Agencies shall implement an Information Security Program required by §2-15-114, MCA, which is aligned and integrated with the security program guidance of the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) Special Publication 800-39 Managing Risk From Information Systems.

IV. Applicability

This Policy applies to agencies, including independent contractors, and other service providers, who have access to or use or manage information subject to the policy and standard provisions of §2-17-534, MCA, unless granted exception as provided in §2-17-515, MCA. The state university system and national guard are exempted from this Policy by §2-17-516, MCA.

V. Scope

This Policy authorizes and requires the implementation of Information Security Program measures for the information systems managed or controlled by agencies in compliance with Title 2, Chapter 17, Part 5 MCA et al, within the context of information security and information technology procurement.

This Policy encompasses information systems for which agencies have administrative responsibility, including systems managed or hosted by third parties on agencies' behalf.

VI. Definitions

Agency	Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA.
Security Program	Organization-wide information security programs address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. Reference NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations, Appendix G Information Security Programs.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.
Information Technology	Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information assurance definitions.

VII. Authorizations, Roles, and Responsibilities

Refer to the Statewide Policy: Essential Information Security Roles for applicable authorization, roles, and responsibilities.

VIII. Requirements

Each agency shall implement its information security program based on National Institute Standards and Technology guidance, utilizing the Risk Management Framework outlined in NIST SP800-39 Managing Risk From Information Systems.

Each agency shall implement its security controls in accordance with the guidelines established within NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations, Appendix G Information Security Programs, and other applicable guidance and publications referenced therein.

Agencies shall use the latest publicly available versions of publications referenced within this Policy *at its date of approval*. (Note: Because newer versions of the publications referenced herein become available from time-to-time, each agency is encouraged to stay current by using

the most recent versions, as deemed feasible by each agency. Future revisions of this Policy shall reference then currently-available versions.)

IX. Compliance

Compliance with this Policy shall be demonstrated by progress on the implementation of the Agency Information Security Program Plan.

X. Change Control and Exceptions

The Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards shall govern policy changes or exceptions. Submit requests for a review or change to this instrument by Action Request form (at http://itsd.mt.gov/content/policy/policies/Administration/action_request.doc). Submit requests for exceptions by an Exception Request form (at http://itsd.mt.gov/content/policy/policies/Administration/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

XI. Closing

Direct questions or comments about this instrument to the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

XII. References

A. Legislation

- Title 2, Chapter 17, Part 5, MCA, et al.
- §2-15-114, MCA Security Responsibilities of Departments for Data.
- §2-17-534, MCA Security Responsibilities of Department.

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

C. Standards, Guidelines

- Guide To NIST Information Security Documents

- NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP800-39, Managing Risk from Information Systems

XIII. Administrative Use

Product ID:	POL-20090701a
Proponent:	Chief Information Officer
Publisher	Office of the Chief Information Officer
Published Date:	March 5, 2010
Version Date:	3/5/2010
Custodian:	Policy Manager
Approved Date:	March 5, 2010
Effective Date:	July 1, 2012
RIM Class:	Record
Disposition Instructions:	For the Record
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this instrument may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2017
Last Review Date:	<None>
Changes:	